AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Currently Amended) A method for authorizing access to a human resources database, comprising:

detecting, by a computer, a new query for a set of database records;

determining whether an identifier associated with the set of database records matches an identifier of a user that submitted the new query;

determining whether [[a]] the user ~~that submitted the new query~~ is authorized to acquire a new lock on the set of database records, wherein the user is authorized if the ~~user does not have a conflict of interest with respect to~~ identifier associated with the set of database records does not match the identifier of the user;

denying the new lock if the user is not authorized; and

setting the new lock or ~~attempting~~ making an attempt to set the new lock if the user is authorized.

2 - 3. (Cancelled).

4. (Previously Presented) The method as recited in claim 1 further comprising informing the user that the user cannot access the set of database records when the user is not authorized.

5. (Previously Presented) The method as recited in claim 1 further comprising permitting access to the set of database records if the user is authorized.

6. (Previously Presented) The method as recited in claim 5 further comprising releasing the new lock after the user has checked out from the set of database records.

7. (Previously Presented) The method as recited in claim 1 wherein determining whether the user is authorized further includes determining whether the user has write authorization for the set of database records.

8. (Previously Presented) The method as recited in claim 1 wherein determining whether the user is authorized further includes determining whether the user has a maximum database access authorization.

9. (Cancelled).

10. (Previously Presented) The method as recited in claim 1 wherein determining whether the user is authorized includes determining whether the user is organizationally authorized.

11. (Previously Presented) The method as recited in claim 1 wherein determining whether the user is authorized includes determining includes whether the user is currently authorized.

12. (Currently Amended) A computer-readable medium storing program instructions for performing a method of authorizing access to a human resources database, the method comprising:

detecting a new query for a set of database records;

determining whether an identifier associated with the set of database records matches an identifier of a user that submitted the new query;

determining whether [[a]] the user ~~that submitted the new query~~ is authorized to acquire a new lock on the set of database, wherein the user is authorized if the ~~user does not have a conflict of interest with respect to~~ identifier associated with the set of database records does not match the identifier of the user;

denying the new lock if the user is not authorized; and

setting the new lock or ~~attempting~~ making an attempt to set the new lock if the user is authorized.

13 - 14. (Cancelled).

15. (Previously Presented) The computer-readable medium recited in claim 12 further comprising the user that the user cannot access the set of database records when the user is not authorized.

16. (Previously Presented) The computer-readable medium as recited in claim 12 further comprising permitting access to the set of database records if the user is authorized.

17. (Previously Presented) The computer-readable medium as recited in claim 16 further comprising releasing the new lock after the user has checked out from the set of database records.

18. (Previously Presented) The computer-readable medium as recited in claim 12 wherein determining whether the user is authorized includes determining whether the user has write authorization for the set of database records.

19. (Previously Presented) The computer-readable medium as recited in claim 12 wherein determining whether the user is authorized includes determining whether the user has a maximum database access authorization.

20. (Currently Amended) The computer-readable medium as recited in claim 12 wherein ~~determining whether~~ the user has a conflict of interest ~~includes determining whether~~ when the set of database records personally pertain to the user.

21. (Previously Presented) The computer-readable medium as recited in claim 12 wherein determining whether the user is authorized includes determining whether the user is organizationally authorized.

22. (Currently Amended) The computer-readable medium as recited in claim 12 wherein determining whether the user is authorized includes determining whether the user is currently authorized.

23 - 24. (Cancelled).

25. (Currently Amended) A database system authorizing access to a human resources database, comprising:

a processor;

a memory storing instructions executable by the processor, the instructions comprising:

means for detecting, by a computer, a new query for a set of database records;

means for determining whether an identifier associated with the set of database records matches an identifier of a user that submitted the new query;

means for determining whether [[a]] the user ~~that submitted the new query~~ is authorized to acquire a new lock on the set of database records, wherein the user is authorized if the ~~user does not have a conflict of interest with respect to~~

identifier associated with the set of database records does not match the identifier of the user;

means for denying the new lock if the user is not authorized; and

means for setting the new lock or ~~attempting~~ making an attempt to set the new lock if the user is authorized.

26 - 27. (Cancelled).

28. (Previously Presented) The database system as recited in claim 25 further comprising means for informing the user that the user cannot access the set of database records when the user is not authorized.

29. (Previously Presented) The database system as recited in claim 25 further comprising means for permitting access to the set of database records if the user is authorized.

30 - 34. (Cancelled).

35. (Currently Amended) A method for making a preliminary determination of whether a user has authorization to access a set of database records, comprising:

detecting, by a computer, a new query from the user for a set of database records;

determining whether an identifier associated with the set of database records matches an identifier of the user that submitted the new query;

determining whether the user has a chance of being authorized to acquire a new lock for the set of database records based on the identifier of the user and at least one of (a) write authorization and (b) a lack of conflict of interest; and

denying the new lock if the user does not have a chance of being authorized.

36. (Currently Amended) The method of claim 35, further comprising:

setting the new lock or ~~attempting~~ making an attempt to set the new lock if the user has a chance of being authorized.

37. (Previously Presented) The method of claim 35, wherein determining whether the user has any chance of being authorized to acquire the new includes determining whether the user has a maximum database access authorization.

38. (Previously Presented) The method of claim 35, wherein determining whether the user has a conflict of interest includes determining whether the set of database records personally pertain to the user.

39. (New) The method of claim 35, further comprising:

determining, when the identifier associated with the set of database records matches the identifier of the user, whether the set of database records comprise critical or non-critical information; and

wherein the user does not have a chance of being authorized when the set of database records comprise critical information.

40. (New) The method of claim 39, wherein the critical information comprises pay records of the user.

41. (New) A method for determining whether a user has authorization to access a set of database records, comprising:

detecting, by a computer, a new query from the user for a set of database records;

determining whether an identifier associated with the set of database records matches an identifier of the user that submitted the new query;

determining whether the user is authorized to acquire a new lock for the set of database records based on the identifier of the user and, when the identifier associated with the set of database records matches the identifier of the user, whether the set of database records comprise critical or non-critical information; and

denying the new lock if the user does not have a chance of being authorized.

42. (New) The method of claim 41, wherein the user is not authorized when the set of database records comprise critical information.

43. (New) The method of claim 42, wherein the critical information comprises pay records of the user.

44. (New) A method for authorizing access to a human resources database, comprising:

detecting, by a computer, a new query for a set of database records;

determining whether an identifier associated with the set of database records matches an identifier of a user that submitted the new query;

determining whether the user is authorized to acquire a new lock on the set of database records, the user being authorized if the user does not have a conflict of interest with respect to the set of database records, wherein the user does not have a conflict of interest when the identifier associated with the set of database records does not match the identifier associated with the user;

denying the new lock if the user is not authorized; and

setting the new lock or making an attempt to set the new lock if the user is authorized.

45. (New) A method for authorizing access to a human resources database, comprising:

detecting, by a computer, a new query for a set of database records;

determining whether a user that submitted the new query is authorized to acquire a new lock on the set of database records, wherein the user is authorized if the user does not have a conflict of interest when the set of database records do not personally pertain to the user;

denying the new lock if the user is not authorized; and

setting the new lock or making an attempt to set the new lock if the user is authorized.